

organization for
applied scientific
research

TNO-report

FEL

Laboratory

P.O. Box 968
2509 JG The **TD**
Oude Waalsdorperweg 97
The Hague The Netherlands
Fax +31 70 328 09 61
Phone +31 70 326 42 21

report no.
FEL-91-B099

copy no.

title

9 **OSI-Security and Relations with other Security
Standards**

AD-A236 339



Nothing from this issue may be reproduced
and/or published by print, photoprint,
microfilm or any other means without
previous written consent from TNO.
Submitting the report for inspection to
parties directly interested is permitted.

In case this report was drafted under
instruction, the rights and obligations
of contracting parties are subject to either
the 'Standard Conditions for Research
Instructions given to TNO' or the relevant
agreement concluded between the contracting
parties on account of the research object
involved.

© TNO

author(s):

P.L. Overbeek

date

March 1991

**DTIC
ELECTE
JUN 07 1991
S B D**

TDCK RAPPORTCENTRALE
Frederikkazerne, Geb. 140
van den Burchlaan 31
Telefoon: 070-3166394/6395
Telefax : (31) 070-3166202
Postbus 90701
2509 LS Den Haag

classification

title	: unclassified
abstract	: unclassified
report text	: unclassified
appendix A	: unclassified

no. of copies	: 25
no. of pages	: 34 (incl. appendix, excl. RDP & distribution list)
appendices	: 1

91-01291



DISTRIBUTION STATEMENT A

Approved for public release;
Distribution Unlimited

TNO

All information which is classified according to
Dutch regulations shall be treated by the recipient in
the same way as classified information of
corresponding value in his own country. No part of
this information will be disclosed to any party.

91 6 5 005

report no. : FEL-91-B099
title : OSI-Security and Relations with other Security Standards
author(s) : P.L. Overbeek
institute : TNO Physics and Electronics Laboratory
date : March 1991
NDRO no. :
no. in pow '91 : 709.2
Research supervised by : D.W. Fikkert, H.A.M. Luijck
Research carried out by : P.L. Overbeek

ABSTRACT (unclassified)

Within NATO it is acknowledged that it is an advantage if standard civil information technology products can be used for military purposes. For this, military security requirements should be met. The OSI Security Architecture addresses only one of the relevant security issues. Other relevant issues are: security in (open) systems, security in distributed applications and secure information technology products. This paper describes the relations of the OSI Security Architecture with other areas of security and other standards in these areas. An emphasis is put on civil standards for the evaluation of security in information technology products.

This study has been performed as part of the PhD-project SEDIS (Securable Distributed Information Systems). This project aims at a better understanding of and contribution to security in distributed information systems.

This paper has been presented at the "Military OSI Symposium", Shape Technical Centre, June 1990.



Accession For	
NTIS GRA&I	<input checked="" type="checkbox"/>
DTIC TAB	<input type="checkbox"/>
Unannounced	<input type="checkbox"/>
Justification	
By	
Distribution/	
Availability Codes	
Dist	Avail and/or Special
A-1	

rapport no. : FEL-91-B099
titel : OSI-Security and Relations with other Security Standards

auteur(s) : ir. P.L. Overbeek
instituut : Fysisch en Elektronisch Laboratorium TNO

datum : maart 1991
hdo-opdr.no. :
no. in iwp '91 : 709.2

Onderzoek uitgevoerd o.l.v. : D.W. Fikkert, ir. H.A.M. Luijff
Onderzoek uitgevoerd door : ir. P.L. Overbeek

=====

SAMENVATTING (ongerubriceerd)

Het voordeel van het gebruik van standaard, commercieel verkrijgbare informatie technologie-producten voor militaire toepassingen wordt door de NAVO onderkend. Gebruik van deze producten is alleen mogelijk als aan specifieke militaire eisen wordt voldaan, met name op beveiligingsgebied. De OSI Security Architecture beschrijft slechts een deel van deze eisen. Andere relevante onderwerpen zijn: security in (open) systems, security in distributed applications en secure information technology products. Deze studie beschrijft de relaties van de OSI Security Architecture met deze onderwerpen en andere beveiligingsstandaarden. Met name wordt ingegaan op civiele standaarden voor de evaluatie van beveiliging in IT-producten. Dit onderzoek is uitgevoerd als onderdeel van het promotieonderzoek SEDIS (Securable Distributed Information Systems). Dit project beoogt inzicht te verwerven in, en bij te dragen aan beveiliging in gedistribueerde informatie systemen. Deze studie is gepresenteerd op het Shape Technical Centre "Military OSI Symposium", Juni 1990.

CONTENTS

ABSTRACT	2
SAMENVATTING	3
CONTENTS	4
1 INTRODUCTION	5
2 OSI AND SECURITY: STATE OF THE ART	6
3 PLACEMENT OF OSI SECURITY WITHIN SYSTEMS SECURITY	7
3.1 Secure open Systems	7
3.2 Security in Distributed Applications	8
3.3 Secure information technology products	8
4 COMPARISON OF 'STANDARDS' FOR SECURITY EVALUATION CRITERIA AND TECHNIQUES IN RELATION TO OSI SECURITY	9
4.1 Canadian Trusted Computer Product Evaluation Criteria (CTCPEC)	9
4.2 United Kingdom: Technical Criteria for the Security Evaluation of IT-products.	10
4.3 Germany: IT-Security Criteria	11
4.4 Recommendations	12
5 CONCLUSIONS	13
6 LITERATURE	14

APPENDIX A PRESENTATION SHEETS

1. INTRODUCTION

Within NATO it is acknowledged that if civil products can be used for military purposes too, a considerable effort in developing special-purpose military solutions can be saved. This is one of the reasons why the trusted communications sublayer between the OSI-layers 3 (network layer) and 4 (transport layer) has been proposed. However, this sublayer is only one part of the security puzzle, since it cannot offer all of the security needs and is only one barrier towards the information. The more secure civil products are, the better they can be used for military purposes. Also for this reason, the OSI Security Architecture is of great importance. However, the most OSI can offer are standards for technical security in networks.

In this paper, the OSI Security Architecture is placed in the perspective of the total of security demands. An emphasis is put on civil standards for the evaluation of security in information technology products with respect to the services in OSI. The aim of this paper is to stress the fact that OSI Security addresses only one of the relevant security issues. Other relevant issues are security in (open) systems, security in distributed applications and secure information technology products. These issues are not independent of each other.

This paper has been written as part of the SEDIS-project (Securable Distributed Information Systems). This project aims at a better understanding of, and contribution to, security in distributed information systems.

2. OSI AND SECURITY: STATE OF THE ART

Within the OSI/IEC/JTC1 subcommittee SC21 (OSI Architecture, Management and Upper Layers) a unifying view towards security standards is promoted. The aim is to assure coherence of all the work done relative to security in open systems. This unifying view will also be a roadmap for the development of other standards. So far, the SC21 work has been concentrated on OSI rather than the broader area of open systems. SC21 recently embraced the view that the OSI Security Architecture is only the first stage in defining security services and mechanisms. For example, the OSI Security Architecture is not an implementation specification. Further standards are required that build upon an architecture. The naming of these standards is: framework, model and technique (major examples in OSI are given between brackets).

- A *Security Architecture* describes generic security services, mechanisms and management functions required in the context of a given environment, as well as their placement in the architecture. [OSI Security Architecture]
- The purpose of the *Security Frameworks* is to provide comprehensive and consistent descriptions of specific functional areas of security. These descriptions will address all aspects of these areas in relation to how they may be applied in the context of a specific security architecture. Generic solutions are defined and consistency between the frameworks of an architecture is ensured. [Frameworks for Authentication, Access Control, Non-Repudiation and Audit in OSI]
- The purpose of the *Security Models* is to apply the security concepts detailed in the Security Frameworks to specific areas. Models detail how and when mechanisms and elements of the frameworks are combined. [Upper and Lower Layer Security Model]
- *Security Techniques* provide building blocks for the implementation of security. [Techniques for Encipherment, Digital Signatures, Hash Functions, Non-Cryptographic Techniques]

In all these areas a lot of work is going on, and the process of standardization evolves thoroughly, but slowly. Strictly speaking, only the OSI Security Architecture is an International Standard. The frameworks are in the Working Draft stage, models are in an early Working Draft stage. Note that for compliance with OSI, the Security Architecture is not obliged.

3. PLACEMENT OF OSI SECURITY WITHIN SYSTEMS SECURITY

OSI can offer at most standards for network security. The OSI Security Architecture does not address issues of end-system (computer) security (secure open systems), security in distributed applications or security within information technology products.

Normally, security is a combination of physical security, organizational/procedural security and (technical) systems security. If one of these falls short, compensation must be found within the others. For example, if there are no possibilities for the technical security of information at the end-systems, additional physical and procedural measures must be taken. If security at the physical environment of the end-systems can be considered adequate, network security through the Trusted Communication Sublayer can fulfil the security requirements with respect to confidentiality of the transported information. Other requirements remain to be fulfilled.

3.1 Secure open Systems

Security at the end-systems is the responsibility of the operating system. Today, security is host-oriented. This means that as long as the information flow or processing is on one end-system, the operating system offers security. These issues are rather well understood. However, the systems of today work in networks and communicate with one another. There is a tendency of dynamic assignment of the actual place of processing and storage of information. This asks for integration of operating systems security and network security.

For the security at the end-systems, it is likely that an other security architecture is needed. ISO/IEC/JTC1 is about to form Subcommittee 27 (one of the proposed names for SC27 is 'IT Security Techniques'). SC27 is likely to be assigned responsibility for this subject under the name Secure Open Systems. Also the European Computer Manufacturers Association (ECMA) has done some work in this direction.

3.2 Security in Distributed Applications

Today, security in distributed applications is offered within the applications themselves. Of course this is a far from ideal solution, because system developers must design and develop solutions for the security problems within their distributed application over and over again. It is desirable if the security is not part of the application. As long as we do not have secure open (operating) systems, a better solution is to provide a common library of security functions with properly defined interfaces, callable by the applications. This also enables data exchange between applications.

SC27 will probably do some work in this area. Some work in this field has already been done within SC21, by working groups as Online Data Processing and Database, as well as groups working on Secure Message Handling System (SC18 'Text and Office Systems'; CCITT), Security in the Directory (CCITT) and Secure EDI (CCITT).

3.3 Secure information technology products

For security in IT-products there existed only one accepted set of security evaluation criteria: the Colored Books of the DoD. Best known in this set is the Orange Book (Trusted Computer System Evaluation Criteria, DoD 5200.28-STD). Lately, a lot of activity is going on in this area. New 'standards' for security evaluation criteria emerge rapidly. The most important sets of evaluation criteria are discussed in some detail later in this paper.

All the issues mentioned above have a direct influence on security. Application, operating systems and network security are all important. They are much more effective when being used in combination and integrated. Again, these security issues are not independent of each other.

4. COMPARISON OF 'STANDARDS' FOR SECURITY EVALUATION CRITERIA AND TECHNIQUES IN RELATION TO OSI SECURITY

The standard for the evaluation of security in computer systems which had the largest impact on the market is undoubtedly the Orange Book. Today, new security needs are identified, which ask for a new (or modified) standard for evaluation criteria. Evaluation criteria for civil usage are being developed by, among others, Canada, the United Kingdom and Germany. The Netherlands, France, Germany and the United Kingdom have planned to develop a common standard.

A comparison can be made of the main evaluation criteria in these standards with the services and mechanisms as defined in the OSI Security Architecture. In this way we can evaluate if an easy mapping between evaluation criteria and OSI services and mechanisms can be made in a specific set of evaluation criteria.

The OSI Security Architecture defines the following services: Authentication, Access Control, Confidentiality, Integrity and Non-Repudiation. The following mechanisms that implement those services are used: Encipherment, Digital Signature, Access Control, Data Integrity, Authentication Exchange, Traffic Padding, Routing Control and Notarization.

4.1 Canadian Trusted Computer Product Evaluation Criteria (CTCPEC)

The May 1989 draft of the CTCPEC is comparable with the Orange Book. For the evaluation of confidentiality, the categories are almost the same (categories A to D). The first main difference is its extension of the Orange Book with respect to evaluation criteria for integrity and availability. The second main difference is that the evaluation of the 'strength' of the security (assurance) is evaluated separate from the existence of a specific security functionality. The evaluation categories are: confidentiality, availability, integrity, accountability and the assurance level of these security aspects.

A typical rating for a system might be:

Confidentiality:	B
Integrity:	F
Availability:	K
Accountability:	P
Trustworthiness:	T2

The Canadian Evaluation Criteria are not applicable to networks. So additional criteria (or interpretations) are needed for the evaluation of security aspects of networks.

4.2 United Kingdom: Technical Criteria for the Security Evaluation of IT-products.

The UK Department of Trade and Industry (DTI) has sponsored the development of Technical Criteria for the evaluation of Information Technology products. These criteria are known as the 'Green Books' (note the plural). Steps have been taken to avoid incompatibility of evaluation and certification schemes between the military and commercial sectors. For the establishment of a *single* scheme, a close relation with the Communications-Electronics Security Group is established. Beside this, there are discussions in progress between UK, France, Germany and the Netherlands concerning common security evaluation criteria.

As is the case with the Canadian proposal, there are two aspects to the consideration of the security capabilities of IT-products: functionality (the features of the product which contribute to the security) and assurance (the confidence that security needs have been satisfied).

The specification of security functionality is considered in two complementary ways: by Security Prerequisites, which are a set of axiomatic statements about security properties in a system, and by a Claims Language. The manufacturers claims are the baseline for evaluation. The aim of the Claims Language is to describe precisely the security features of a product in a standard way. These are the claims that will be evaluated. So far there is insufficient experience to say whether it is just a nice idea or it is really practical.

The Green Books also address many important issues that are outside the scope of this paper: software lifecycle, development criteria and the vendor's background and behaviour.

The security prerequisites are important in the comparison with the OSI Security Architecture. There are two kinds of prerequisites: those that are enforceable (Security Control) and those that are not (Security Objective). The first kind needs preventive, the second detective measures.

The following Security Controls are defined: accountability, authentication, permission, object protection, object reuse, no repudiation. The Security Objectives are: no addition, no loss, confinement, timeliness, no denial of resource.

An evaluation of a product consist of a long list with the manufacturers claims and the evaluation level of that claim. An evaluation level of L1 indicates that the claim must not be trusted, L6 indicates a high confidence in the claim.

Although it is not impossible, it is difficult to map these prerequisites with the services and mechanisms of the OSI Security Architecture. To do this, an 'interpretation' guide would be needed.

4.3 Germany: IT-Security Criteria

The German "Criteria for the Evaluation of Trustworthiness of Information Technology Systems" (1st version 1989) are published by the German Information Security Agency (GISA) on behalf of the Government. These criteria, also known as the Green Book (no plural), are a further development of the Orange Book-criteria.

The following 'basic security functions' are defined: authentication, administration of rights, audit, object reuse, error recovery, continuity of service and data communication security(!).

As is the case with the Canadian and UK schemes, there is a rating for the assurance of the security that is offered by an implementation of a basis security function (Q0 to Q7).

To describe the kind of security that is offered, classes of functionality are defined. The number of classes of functionality is not limited, although at this moment only 10 classes are defined. The first five are direct mappings of the Orange Book classes. For example, the criteria in functionality class 'F1' are equal with the Orange Book 'C1'-criteria.

The other functionality classes defined so far are:

- F6 High integrity for data and programs
- F7 High availability
- F8 High integrity during data communication
- F9 High confidentiality during data communication
- F10 Integrity and confidentiality demands in networks

A typical rating for a system might be:

(F2, Q3) and (F6, Q2) and (F8, Q4)

For the characterization of the protection mechanisms for data communications, the OSI Security Architecture is used. Although many aspects are not very clear yet, this is a great advantage of the German proposal.

The classes of functionality are treated independently. This is not without disadvantages. As a result it must be accepted that areas of overlap exist between functionality classes. Moreover, it is not clear what a F5 (=Orange Book A1) with assurance level Q0 (= inadequate assurance) might mean. Secondly, a separation of network and operating system security in the functionality classes gives rise to interface problems between the network and the operating systems. A secure network can securely transport information between secure end-systems. However, the end-systems have no means to know whether they can trust each other.

4.4 Recommendations

Of course, it is desirable that only one standard for security evaluation criteria and techniques remains for civil usage. If a military version is needed, it ought to be an extension of this civil standard.

In a standard for security evaluation criteria, security of networking must be covered also. To prevent interpretation problems, the terminology of the OSI Security Architecture should be adopted (services and mechanisms).

The discussion about the civil standard must be international. The ISO is the best suited place for this discussion. According to its current name 'IT Security Techniques', this work can be allotted to SC27.

5. CONCLUSIONS

OSI Security is evolving slowly but thoroughly. OSI offers at most network security. This is only one of the relevant security issues. Other issues are: security in operating systems and security in distributed information systems. These issues are not independent of each other. Security is most effective if network and operating system security are integrated.

The development of a common standard for IT Security Evaluation Criteria and Techniques must be encouraged. The services and mechanisms of the OSI Security Architecture must be present in this standard. The discussion about the civil standard must be international. The ISO seems to be the proper place for this, especially SC27. If a military version is needed, a military standard for IT Security Evaluation Criteria and Techniques should be an extension of the civil standard.

6. LITERATURE

ISO/IEC/JTC1/SC21 N4258: Working draft for a Guide to Open System Security

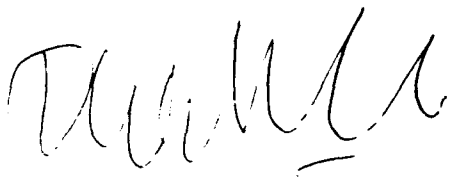
Canadian Trusted Computer Product Evaluation Criteria, version 1.0 DRAFT, may 1989 - System

Security Centre, Communications Security Establishment, Government of Canada

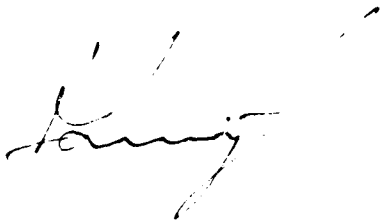
'Green Books', The Security of IT Systems and Products, 7 volumes, DRAFT, 1989, available
from UK DTI Industry Commercial Computer Security Centre.

IT-Security Criteria, Criteria for the Evaluation of Trustworthiness of Information Technology
Systems, 1st version 1989, ISBN 3-88784-200-6

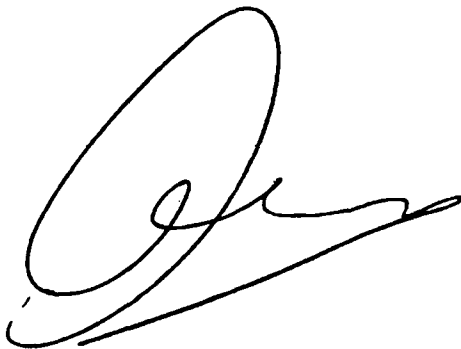
Trusted Computer System Evaluation Criteria, DoD 5200.28-STD



D.W. Fikkert
(projectleader)



Ir. H.A.M. Luijff
(supervisor)



Ir. P.L. Overbeek
(author)

PRESENTATION SHEETS

Deze bijlage bevat 18 sheets.

This appendix contains 18 sheets.

OSI Security and relations with other security standards

Paul Overbeek
TNO Physics and Electronics Laboratory
The Netherlands

Information Security
Networks

SEDIS

OSI Security and relations with other security standards

Contents

- 1 Introduction
- 2 State of the art
- 3 Placement of OSI-Security within systems security
- 4 Evaluation Criteria
- 5 Conclusions and Recommendations

Introduction

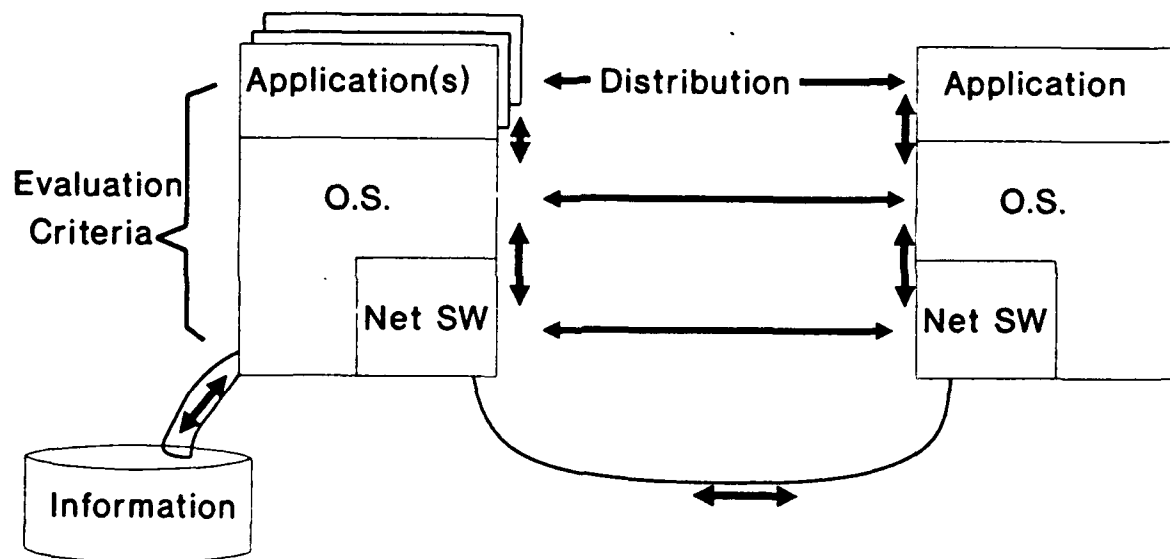
Civil products for military purposes?

has advantages...
but...

Are they secure?

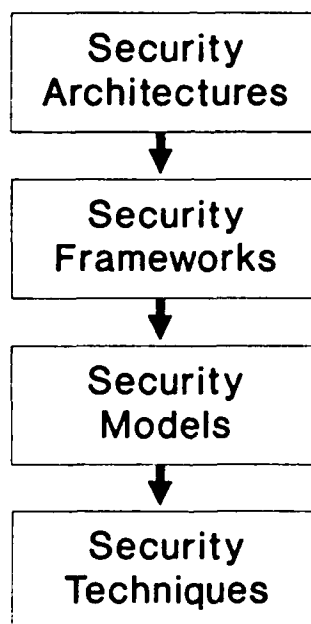
Stimulate security in (civil) products

Security areas of concern

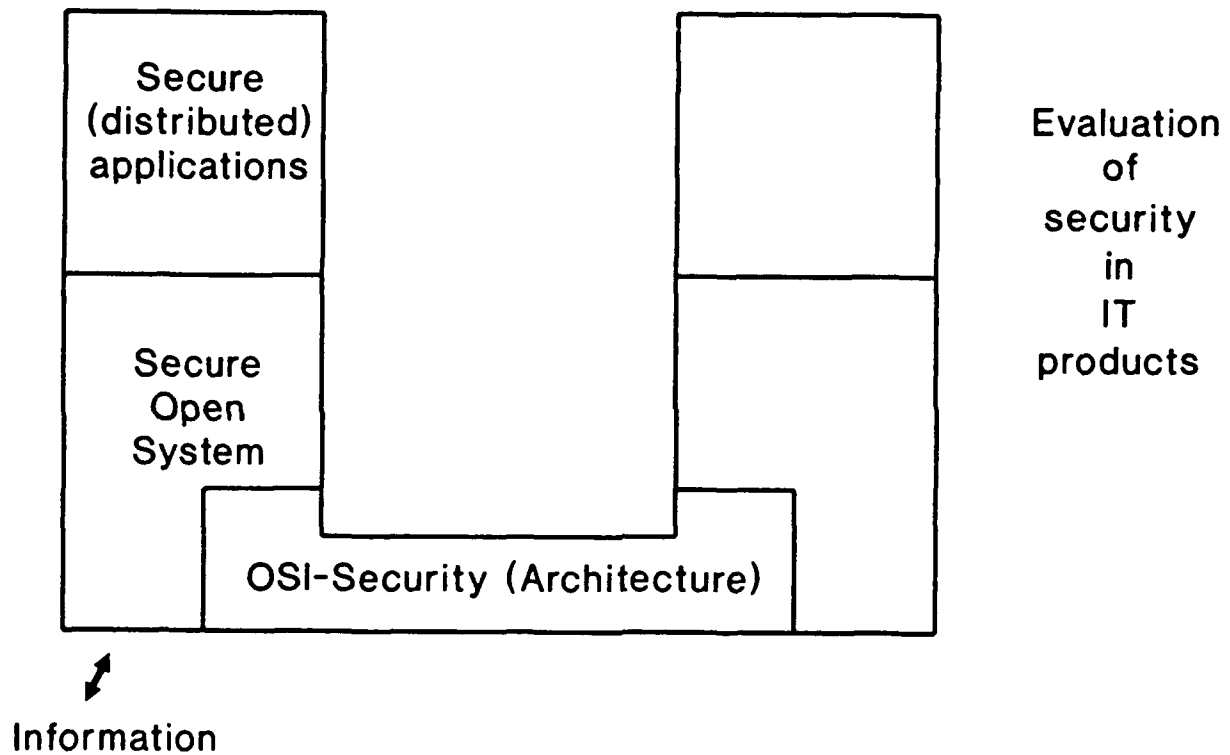


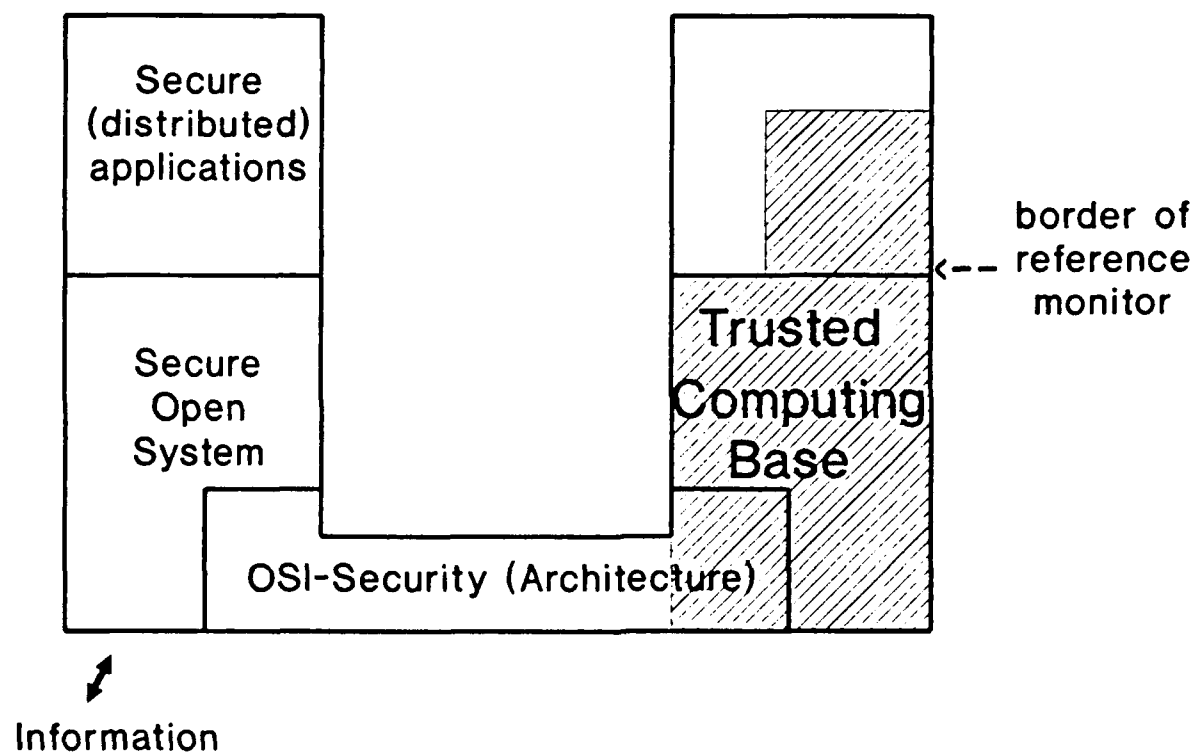
Mutual dependency

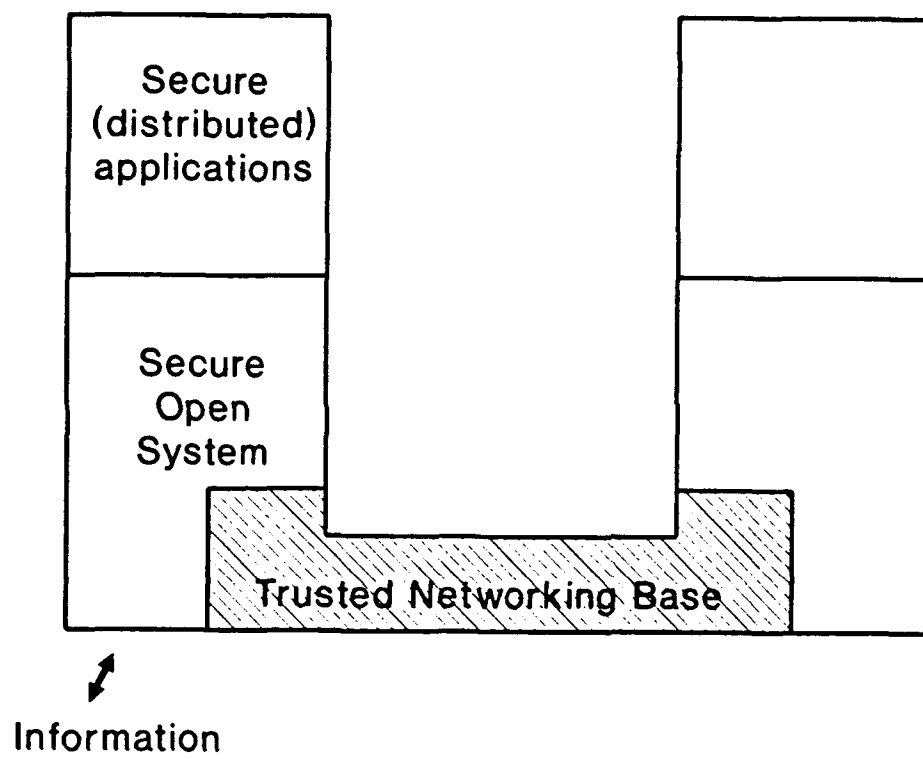
Unifying view towards standards SC21

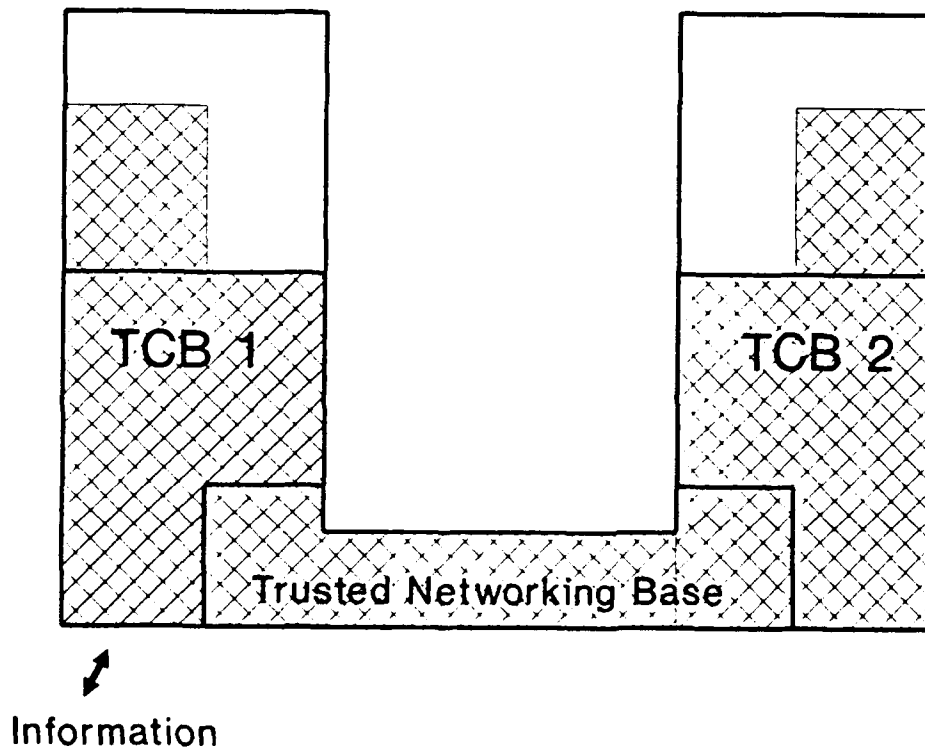


Placement of OSI-Security









Security Evaluation Criteria and Techniques

Background:

- New security needs
- Demand for refined approach

Many initiatives

- Canadian
 - UK
 - German
 - 'European'
- and many more

Comparison of Criteria

- Basis for evaluation
- Mapping with the Orange Book
- Suitable for networks,
mapping with (services in) OSI Security Architecture:
 - authentication
 - access control
 - confidentiality
 - integrity
 - non repudiation

Canada: Trusted Computer Product Evaluation Criteria (CTCPEC)

Evaluation of functionality:

- Confidentiality
- Integrity
- Availability
- Accountability

Assurance:

- Trustworthiness

Easy mapping with the Orange Book

Extension or interpretation needed for networks

Typical rating: C2, E, K, T2

UK Technical Criteria for the Evaluation of IT-products

Evaluation of functionality and assurance

Functionality: security prerequisites:

- Security controls (enforceable):
accountability, authentication, permission,
object protection, reuse, no repudiation
- Security Objectives:
no addition, no loss, confinement,
no denial of resources, timeliness

Assurance: 6 evaluation levels

Claims language: basis for evaluation

UK Technical Criteria for the Evaluation of IT-products

- No direct mapping with Orange Book
- No easy mapping with OSI Security Architecture

German Criteria for the Evaluation of Trustworthiness of IT-systems

Functionality: basic security functions:
authentication, administration of rights, audit,
object reuse, recovery, continuity and ...
data communications security

Assurance level

Classes of functionality:

F1 to F5 = orange book C1 to B3/A1

..

F10 = Integrity and Confidentiality in Networks
evaluation based on OSI Security Architecture

Typical rating: (F2, Q3) and (F6, Q2) and (F8, Q4)

Terminology differs from Orange Book and OSI SA

'European' Criteria

UK, Germany, France, the Netherlands, (EC)

Call for comments on early draft

Best of both worlds --> rather complex

Orange Book and OSI Security Architecture

Looks promising

Conclusions and Recommendations

Evaluation Criteria

For military purposes:

- promote a common civil set criteria
'compatible' with Orange Book
including OSI Security Architecture

How:

- via local initiatives
stimulate collaboration
'European' set
- bring subject to OSI SC27 (and make it a normal standard)

IF a military set is needed:

extension to common civil set

Conclusions and Recommendations

OSI Security Architecture is only the first step

Security also dependent on

- Operating System Security
- Application Security

Subjects cannot be treated independently

HOW ARE WE GOING TO EVALUATE ?

Techniques for evaluation?

REPORT DOCUMENTATION PAGE

(MOD-NL)

1. DEFENSE REPORT NUMBER (MOD-NL)	2. RECIPIENT'S ACCESSION NUMBER	3. PERFORMING ORGANIZATION REPORT NUMBER
TD91-2008	—	FEL-91-B099
4. PROJECT/TASK/WORK UNIT NO.	5. CONTRACT NUMBER	6. REPORT DATE
20555		MARCH 1991
7. NUMBER OF PAGES	8. NUMBER OF REFERENCES	9. TYPE OF REPORT AND DATES COVERED
35 (INCL. RDP & 1 APPENDIX, EXCL. DISTRIBUTION LIST)	5	FINAL REPORT
10. TITLE AND SUBTITLE OSI-SECURITY AND RELATIONS WITH OTHER SECURITY STANDARDS		
11. AUTHOR(S) P.L. OVERBEEK		
12. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) TNO PHYSICS AND ELECTRONICS LABORATORY, P.O. BOX 96864, 2509 JG THE HAGUE OUDE WAALSDORPERWEG 63, THE HAGUE, THE NETHERLANDS		
13. SPONSORING/MONITORING AGENCY NAME(S)		
14. SUPPLEMENTARY NOTES		
15. ABSTRACT (MAXIMUM 200 WORDS, 1044 POSITIONS) WITHIN NATO IT IS ACKNOWLEDGED THAT IT IS AN ADVANTAGE IF STANDARD CIVIL INFORMATION TECHNOLOGY PRODUCTS CAN BE USED FOR MILITARY PURPOSES. FOR THIS, MILITARY SECURITY REQUIREMENTS SHOULD BE MET. THE OSI SECURITY ARCHITECTURE ADDRESSES ONLY ONE OF THE RELEVANT SECURITY ISSUES. OTHER RELEVANT ISSUES ARE: SECURITY IN (OPEN) SYSTEMS, SECURITY IN DISTRIBUTED APPLICATIONS AND SECURE INFORMATION TECHNOLOGY PRODUCTS. THIS PAPER DESCRIBES THE RELATIONS OF THE OSI SECURITY ARCHITECTURE WITH OTHER AREAS OF SECURITY AND OTHER STANDARDS IN THESE AREAS. AN EMPHASIS IS PUT ON CIVIL STANDARDS FOR THE EVALUATION OF SECURITY IN INFORMATION TECHNOLOGY PRODUCTS. THIS STUDY HAS BEEN PERFORMED AS PART OF THE PHD-PROJECT SEDIS (SECURABLE DISTRIBUTED INFORMATION SYSTEMS). THIS PROJECT AIMS AT A BETTER UNDERSTANDING OF AND CONTRIBUTION TO SECURITY IN DISTRIBUTED INFORMATION SYSTEMS. THIS PAPER HAS BEEN PRESENTED AT THE "MILITARY OSI SYMPOSIUM", SHAPE TECHNICAL CENTRE, JUNE 1990.		
16. DESCRIPTORS INFORMATION SYSTEMS SECURITY DISTRIBUTED NETWORKS		IDENTIFIERS
17a. SECURITY CLASSIFICATION (OF REPORT) UNCLASSIFIED	17b. SECURITY CLASSIFICATION (OF PAGE) UNCLASSIFIED	17c. SECURITY CLASSIFICATION (OF ABSTRACT) UNCLASSIFIED
18. DISTRIBUTION/AVAILABILITY STATEMENT UNLIMITED		17d. SECURITY CLASSIFICATION (OF TITLES) UNCLASSIFIED